

**IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION**

TONY BUTLER JR., on behalf of himself and  
all others similarly situated,

Plaintiff,

v.

TRINITY UNIVERSAL INSURANCE  
COMPANY,

Defendant.

Case No.: 3:24-cv-00602

**DEMAND FOR A JURY TRIAL**

**CLASS ACTION COMPLAINT**

Plaintiff Tony Butler Jr. (“Plaintiff”) brings this Class Action Complaint (“Complaint”) against Trinity Universal Insurance Company (“TUIC” or “Defendant”) as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels’ investigation, and upon information and belief as to all other matters, as follows:

**SUMMARY OF ACTION**

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal identifiable information (“PII”) of its customers.
2. Defendant is a company that offers insurance services to its customers.
3. Plaintiff’s and Class Members’ sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. TUIC collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined below), who are (or were) customers at Defendant.

5. The PII compromised in the Data Breach was exfiltrated by criminals and remains in the hands of those criminals who target PII for its value to identity thieves.

6. As a result of the Data Breach, Plaintiff and Class Members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

7. The Data Breach was a direct result of Defendant's failure to properly encrypt, redact, and remove former consumers' PII that it was no longer required to maintain from its data-management systems.

8. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure the PII it collected was adequately encrypted, redacted, and/or protected from physical theft, by failing to implement a comprehensive written information security program that contains

reasonable administrative, technical, and physical safeguards, and by failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized removal by an unknown third party and precisely what specific type of information was accessed.

14. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

15. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

### **JURISDICTION AND VENUE**

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because its principal place of business is in the Dallas Division of the Northern District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

18. Venue is proper under 18 U.S.C. § 1391(b)(1) because Defendant's principal place of business is in the Dallas Division of the Northern District of Texas and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

### **PARTIES**

19. Plaintiff Tony Butler Jr. is a resident and citizen of Tenino, Washington.

20. Defendant is a company organized under the state laws of Texas with its principal place of business located at 12790 Merit Dr., Suite 400, Dallas, Texas 75251. It is a citizen of Texas.

## **FACTUAL ALLEGATIONS**

### ***Defendant's Business***

21. Defendant is a company that offers insurance services to its customers.

22. Plaintiff and Class Members are current and former customers at Defendant.

23. In the course of their relationship, customers, including Plaintiff and Class Members, provided Defendant with at least the following: names, dates of birth, and Social Security numbers.

24. Upon information and belief, in the course of collecting PII from customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

25. Plaintiff and the Class Members, as customers at Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their PII, especially when their Social Security numbers and other sensitive PII is involved.

### ***The Data Breach***

26. On or about February 9, 2024, Defendant began sending Plaintiff and other Data Breach victims an untitled letter (the "Notice Letter"), informing them that:

TUIC recently completed an investigation into an incident involving backup tapes that went missing from a TUIC office that was in the process of moving to another location. These backup tapes were contained in a padlocked case ("lockbox") and went missing sometime between July 7, 2023 and July 10, 2023. Immediately upon learning of the issue, we began an investigation and attempted to locate the lockbox, but were unsuccessful. We also notified law enforcement. We conducted a comprehensive review of the data that could have been contained on the backup tapes, which involved a time- and labor-intensive

effort to reconstruct, search and review the data, and, on January 10, 2024, determined that a file contained your name and Social Security number and date of birth.<sup>1</sup>

27. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

28. The attacker acquired backup files that contained the unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

29. Defendant had obligations created by the FTC Act, the Gramm-Leach-Bliley Act, contract, common law, and industry standards to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

30. Plaintiff further believes that his PII and that of Class Members was subsequently sold on the dark web following the Data Breach.

***Defendant Acquires, Collects, And Stores Its Customers' PII***

31. Defendant acquires, collects, and stores a massive amount of PII on its current and former customers.

32. As a condition of obtaining products and/or services at Defendant, Defendant requires that customers and other personnel entrust it with highly sensitive personal information.

33. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

---

<sup>1</sup> The "Notice Letter". A sample copy is available at <https://oag.ca.gov/ecrime/databreach/reports/sb24-580830>

34. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendant absent a promise to safeguard that information.

35. Upon information and belief, in the course of collecting PII from customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security. Including physical safeguards, for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

36. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

***Defendant Knew, Or Should Have Known, of the Risk Because Insurance Companies In Possession Of PII Are Particularly Susceptible To Data Breaches***

37. Data breaches, including those perpetrated against insurance companies that maintain PII in their systems, have become widespread.

38. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.<sup>2</sup>

39. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by criminals.

---

<sup>2</sup> See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

40. Defendant knew and understood unprotected or exposed PII in the custody of insurance companies, like Defendant, is valuable and highly sought after by nefarious parties seeking to illegally monetize that PII through theft or unauthorized access.

41. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would result if a Data Breach occurred, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

42. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

43. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

44. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

45. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

46. As an insurance company in custody of the PII of its customers, Defendant knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and Class



Members, and of the foreseeable consequences if a Data Breach occurred. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate data security measures to prevent the Data Breach, including by implementing reasonable administrative, technical, and physical safeguards.

***Value Of Personally Identifying Information***

47. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”<sup>3</sup> The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”<sup>4</sup>

48. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.<sup>5</sup>

49. For example, Personal Information can be sold at a price ranging from \$40 to \$200.<sup>6</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>7</sup>

---

<sup>3</sup> 17 C.F.R. § 248.201 (2013).

<sup>4</sup> *Id.*

<sup>5</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

<sup>6</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

<sup>7</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

50. Moreover, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>8</sup>

51. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>9</sup>

---

<sup>8</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>

<sup>9</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names.

54. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>10</sup>

55. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

56. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>11</sup>

---

<sup>10</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

<sup>11</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

57. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

***Defendant Fails To Comply With FTC Guidelines***

58. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established data security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt sensitive information; and implement policies to correct any security problems.<sup>12</sup>

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized removal of confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

61. These FTC enforcement actions include actions against insurance companies, like Defendant.

---

<sup>12</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)

62. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

63. Defendant failed to properly implement basic physical and data security practices.

64. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized removal for the PII of its customers or to comply with applicable industry standards and consumer expectations constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

65. Upon information and belief, TUIC was at all times fully aware of its obligation to protect the PII of its customers, TUIC was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it collected and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

***Defendant Fails to Comply with Gramm-Leach-Bliley Act***

66. TUIC is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

67. The GLBA defines a financial institution as “any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956].” 15 U.S.C. § 6809(3)(A).

68. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant

time period Defendant were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

69. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on October 28, 2014.

70. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

71. Both the Privacy Rule and Regulation P require financial institutions to provide consumers with an initial and annual privacy notice. These privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution’s security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to

receive actual notice.” 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

72. Upon information and belief, Defendant failed to provide annual privacy notices to consumers after the relationship ended, despite retaining these consumers’ PII and storing that PII on Defendant’s network systems.

73. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards’ key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of consumer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

74. As alleged herein, Defendant violated the Safeguard Rule.

75. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of consumer information.

76. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

***Common Injuries & Damages***

77. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized parties to abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

***Data Breaches Increase Victims' Risk Of Identity Theft***

78. The unencrypted PII of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

79. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiff and Class Members.



80. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

81. Plaintiff's and Class Members' PII is of great value to hackers and criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

82. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.<sup>13</sup>

83. With "Fullz" packages, criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

84. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

---

<sup>13</sup> "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/)

information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

85. The existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like insurance information) of Plaintiff and the other Class Members.

86. Thus, even if certain information (such as insurance information) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

87. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

***Loss Of Time To Mitigate Risk Of Identity Theft & Fraud***

88. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

89. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiff and Class Members to take the following measures to protect themselves: “be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.”<sup>14</sup>

---

<sup>14</sup> Notice Letter.

90. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

91. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."<sup>15</sup>

92. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>16</sup>

93. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."<sup>[4]</sup>

***Diminution of Value of PII***

---

<sup>15</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

<sup>16</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>

94. PII is a valuable property right.<sup>17</sup> Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

95. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>18</sup>

96. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>19</sup>

97. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.<sup>20,21</sup>

98. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>22</sup>

99. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss.

---

<sup>17</sup> See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> ("GAO Report").

<sup>18</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

<sup>19</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

<sup>20</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

<sup>21</sup> <https://datacoup.com/>

<sup>22</sup> <https://digi.me/what-is-digime/>

Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

100. At all relevant times, TUIC knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if a Data Breach occurred at Defendant, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

101. The fraudulent activity resulting from the Data Breach may not come to light for years.

102. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

103. TUIC was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to more than twenty thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

104. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

***Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary***

105. Given the type of targeted attack in this case and the type of PII involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to

launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

106. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

107. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

108. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

***Loss Of Benefit Of The Bargain***

109. Furthermore, Defendant's poor data security practices deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

***Plaintiff Tony Butler Jr.'s Experience***

110. Plaintiff Tony Butler Jr. is a former TUIC customer.

111. As a condition of obtaining products and/or services at TUIC, he was required to provide his PII to Defendant, including his name, date of birth, and Social Security number.

112. At the time of the Data Breach—approximately July 7, 2023 through July 10, 2023—Defendant retained Plaintiff’s PII in its system.

113. Plaintiff Butler Jr. is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant’s lax data security policies.

114. Plaintiff Tony Butler Jr. received the Notice Letter, by U.S. mail, directly from Defendant, dated February 9, 2024. According to the Notice Letter, Plaintiff’s PII was improperly removed and obtained by an unauthorized party, including his name, date of birth, policy number, and Social Security number.

115. As a result of the Data Breach, and at the direction of Defendant’s Notice Letter, which instructs Plaintiff to “be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity[.]”<sup>23</sup> Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

116. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or

---

<sup>23</sup> Notice Letter.

diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized parties to abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

117. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

118. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

119. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

120. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

121. Plaintiff Tony Butler Jr. has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

### **CLASS ALLEGATIONS**



122. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

123. The Class that Plaintiff seeks to represent is defined as follows:

**Nationwide Class**

All individuals residing in the United States whose PII was removed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in February 2024 (the “Class”).

124. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

125. Plaintiff reserves the right to amend the definition of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

126. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals impacted in the Data Breach is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted in the Data Breach. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

127. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the

questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized parties;
- c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

- k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

128. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

129. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenges of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

130. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intend to prosecute this action vigorously.

131. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and

expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

132. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

133. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

134. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

135. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper

notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

136. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

137. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

## **CAUSES OF ACTION**

### **COUNT I** **Negligence**

**(On Behalf of Plaintiff and the Class)**

138. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 137, as if fully set forth herein.

139. Defendant requires its customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its products and/or services.

140. Defendant collected the PII of Plaintiff and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

141. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

142. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

143. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

144. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data and failing to implement a

comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards

145. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

146. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that it enacted reasonable physical safeguards to adequately protect the PII.

147. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between TUIC and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted TUIC with their confidential PII, a necessary part of being customers at Defendant.

148. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards and consumer expectations to protect confidential PII.

149. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

150. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

151. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

152. Defendant breached its duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII, including failing to implement a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards. The specific negligent acts and omissions committed by Defendant include Defendant's failure to properly encrypt, redact, and remove former consumers' PII that it was no longer required to maintain from its data-management systems and failure to implement appropriate physical safeguards to prevent the unauthorized acquisition of PII.

153. Defendant violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

154. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

155. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

156. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.



157. A breach of security, unauthorized removal, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and failure to implement reasonable administrative, technical, and physical safeguards.

158. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of data breaches in the insurance industry.

159. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

160. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored by Defendant.

161. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

162. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

163. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

164. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

165. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

166. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

167. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and removed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

168. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized parties to abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

169. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which

remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

170. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

171. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security practices; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT II**  
**Negligence *Per Se***  
**(On Behalf of Plaintiff and the Class)**

172. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 137, as if fully set forth herein.

173. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate data security practices to safeguard Plaintiff's and Class Members' PII, including to implement appropriate physical safeguards to prevent the unauthorized acquisition of PII.

174. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of consumer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

175. Defendant breached its duties to Plaintiff and Class Members under the FTCA and GLBA by failing to properly encrypt, redact, and remove former consumers' PII that it was no

longer required to maintain from its data-management systems and by failing to implement a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

176. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

177. Plaintiff and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

178. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

179. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendant knew or should have known that if it failed to meet its duties that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

180. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

**COUNT III**  
**Breach Of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

181. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 137, as if fully set forth herein.

182. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of obtaining products and/or services at Defendant.

183. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

184. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

185. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

186. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

187. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

188. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized removal or disclosure.

189. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

190. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

191. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

192. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

193. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to implement appropriate safeguards to prevent the unauthorized acquisition of PII, including administrative and physical safeguards.

194. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

195. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to properly encrypt, redact, and remove former consumers' PII that it was no longer required to maintain from its data-management systems.

196. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

197. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

198. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security practices; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT IV**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class)**

199. Plaintiff re-alleges and incorporates by reference all the allegations contained in paragraphs 1 through 137, as if fully set forth herein.

200. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

201. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid Defendant and/or its agents for products and/or services and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the products and/or services that were the subject of the transaction and should have had their PII protected with adequate data security.

202. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

203. Defendant failed to properly encrypt, redact, and remove former consumers' PII that it was no longer required to maintain from its data-management systems and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

204. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained products and/or services at Defendant.

205. Plaintiff and Class Members have no adequate remedy at law.

206. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

207. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized parties to abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

208. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by



establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

209. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grants the following:

- A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
  - ii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

- iii. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;
  - iv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

**JURY TRIAL DEMANDED**

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: March 12, 2024

Respectfully Submitted,

By: /s/ Joe Kendall  
JOE KENDALL  
Texas Bar No. 11260700  
**KENDALL LAW GROUP, PLLC**  
3811 Turtle Creek Blvd., Suite 825  
Dallas, Texas 75219  
214-744-3000  
214-744-3015 (Facsimile)  
jkendall@kendalllawgroup.com

Gary M. Klinger\*  
**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN PLLC**  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60606  
Phone: (866) 252-0878  
gklinger@milberg.com

*Attorneys for Plaintiff and  
Proposed Class Counsel*

*\*Pro Hac Vice application forthcoming*